IN THE CLAIMS

1. (Currently Amended) A method for monitoring computer software comprising:

receiving an assertion from an executing process, wherein the executing process is part of ~~integral to~~ an operating system and wherein receiving an assertion comprises:

receiving an assertion request;

performing at least one of:

recognizing an assertion request type corresponding to the assertion request; or

determining a component that sourced the assertion request; and

accepting the assertion request for at least one of:

an assertion request of an enabled recognized assertion request type; or

an assertion request of a determined component which has assertion requests enabled;

recording the assertion when the assertion is violated; and

allowing the executing process to continue execution.

2-3. (Canceled)

4. (Previously Presented) The method of Claim 1 wherein recording the assertion comprises recording a datum that includes at least one of:

type of assertion,

sequence number of the assertion,

time at which the assertion occurred,

identification of processor that produced the assertion,

identification of process that produced the assertion,

identification of the thread that produced the assertion,

text of the assertion,

stack trace,

source line containing the assertion, or

file name of the source containing the code that generated the assertion.

5. (Original) The method of Claim 1 wherein recording the assertion comprises writing information regarding the assertion violation to a computer readable medium.

6. (Original) The method of Claim 1 wherein recording the assertion comprises writing information regarding the assertion violation to a circular buffer.

7. (Original) The method of Claim 1 further comprising:

accepting a command from at least one of a control console and a network connection; and

updating an enable condition for an assertion class according to the command.

8. (Original) The method of Claim 1 further comprising generating an error report according to the recorded assertion.

9. (Original) The method of Claim 8 further comprising dispatching the error report to a realtime assertion monitor.

10. (Previously Presented) The method of Claim 8 wherein generating an error report comprises:

retrieving an assertion violation parameter including at least one of:

type of assertion,

sequence number of the assertion,

time at which the assertion occurred,

identification of processor that produced the assertion,

identification of process that produced the assertion,

identification of the thread that produced the assertion,

text of the assertion,

stack trace,

source line containing the assertion, or

file name of the source containing the code that generated the assertion; and

generating a report file comprising page description statements according to the assertion parameter.

11. (Currently Amended) An apparatus for monitoring computer software comprising:
a memory comprising:
an assertion receiver arranged to receive an assertion from an executing process,
wherein the executing process is part of ~~integral to~~ an operating system
and wherein the assertion receiver comprises:
an assertion request receiver arranged to receive an assertion request; and
an assertion accept determination unit arranged to recognize an assertion type and generate an accept assertion signal for at least one of:
an enabled recognized assertion type; or
an enabled determined component; and
an assertion recorder arranged to record the assertion when the assertion is violated.

12-13. (Canceled)

14. (Previously Presented) The apparatus of Claim 11 wherein the assertion recorder is capable of recording a datum that includes at least one of:
type of assertion,
sequence number of the assertion,
time at which the assertion occurred,
identification of processor that produced the assertion,
identification of process that produced the assertion,
identification of the thread that produced the assertion,
text of the assertion,
stack trace,
source line containing the assertion, or
file name of the source containing the code that generated the assertion.

15. (Previously Presented) The apparatus of Claim 11 wherein the assertion recorder comprises:

an information interface arranged to receive assertion violation data; and

a media controller arranged to convey the assertion violation data to a computer readable medium.

16. (Previously Presented) The apparatus of Claim 11 wherein the assertion recorder comprises:

an information interface arranged to receive assertion violation data; and

a buffer manager arranged to convey the assertion violation data to a circular buffer.

17. (Previously Presented) The apparatus of Claim 11 further comprising:

a command receiver arranged to accept a command from at least one of a control console or a network connection; and

an assertion manager arranged to update an enable condition for an assertion class according to the command.

18. (Previously Presented) The apparatus of Claim 11 further comprising an error report generator arranged to generate an error report according to the recorded assertion.

19. (Previously Presented) The apparatus of Claim 18 further comprising a dispatch unit arranged to dispatch an error report to a real-time assertion monitor.

20. (Previously Presented) The apparatus of Claim 18 wherein the error report generator comprises:

a data retrieval unit that retrieves an assertion violation parameter including at least one of:

type of assertion,

sequence number of the assertion,

time at which the assertion occurred,

identification of processor that produced the assertion,

identification of process that produced the assertion,

identification of the thread that produced the assertion,

text of the assertion,

stack trace,

source line containing the assertion, or

file name of the source containing the code that generated the assertion; and

a report file generator arranged to generate a report file comprising page description statements according to the assertion parameter.

21. (Currently Amended) A computer software monitoring system comprising:

memory capable of storing instructions;

processor capable of executing instructions stored in the memory; and

software monitor instruction sequence that, when executed by the processor, minimally causes the processor to:

receive an assertion from an executing process, wherein the executing process is part of ~~integral to~~ an operating system and wherein the software monitor instruction sequence comprises an assertion receiver instruction sequence that, when executed by the processor, minimally causes the processor to receive an assertion by minimally causing the processor to:

receive an assertion request;

perform at least one of:

recognize a type for the assertion request; or

determine a component that sourced the assertion request; and

accept the assertion request for at least one of:

an enabled recognized assertion request type; or

an enabled determined component,

record the assertion, and

allow the executing process to continue execution.

22-23. (Canceled)

24. (Previously Presented) The computer software monitoring system of Claim 21 wherein the software monitor instruction sequence comprises an assertion recorder instruction sequence that, when executed by the processor, minimally causes the processor to record an assertion by minimally causing the processor to record a datum that includes at least one of:

type of assertion,

sequence number of the assertion,

time at which the assertion occurred,

identification of processor that produced the assertion,

identification of process that produced the assertion,

identification of the thread that produced the assertion,

text of the assertion,

stack trace,

source line containing the assertion, or

file name of the source containing the code that generated the assertion.

25. (Original) The computer software monitoring system of Claim 21 wherein the software monitor instruction sequence comprises an assertion recorder instruction sequence that, when executed by the processor, minimally causes the processor to record an assertion by minimally causing the processor to write information regarding the assertion to a computer readable medium.

26. (Original) The computer software monitoring system of Claim 21 wherein the software monitor instruction sequence comprises an assertion recorder instruction sequence that, when executed by the processor, minimally causes the processor to record an assertion by minimally causing the processor to write information regarding the assertion to a circular buffer.

27. (Previously Presented) The computer software monitoring system of Claim 21 wherein the software monitor instruction sequence further minimally causes the processor to:

accept a command from at least one of a control console or a network connection; and

update an enable condition for an assertion class according to the command.

28. (Original) The computer software monitoring system of Claim 21 wherein the software monitor instruction sequence further minimally causes the processor to generate an error report according to the recorded assertion.

29. (Original) The computer software monitoring system of Claim 28 wherein the software monitor instruction sequence further minimally causes the processor to dispatch the error report to a real-time assertion monitor.

30. (Previously Presented) The computer software monitoring system of Claim 28 wherein the software monitor instruction sequence comprises an error report generator instruction sequence that, when executed by the processor, minimally causes the processor to generate an error report by minimally causing the processor to:

retrieve an assertion violation parameter including at least one of:

type of assertion,

sequence number of the assertion,

time at which the assertion occurred,

identification of processor that produced the assertion,

identification of process that produced the assertion,

identification of the thread that produced the assertion,

text of the assertion,

stack trace,

source line containing the assertion, or

file name of the source containing the code that generated the assertion; and

generate a report file comprising page description statements according to the assertion parameter.

31. (Currently Amended) A computer-readable medium having computer-executable instructions for performing a method for monitoring computer software, the instructions comprising modules for:

receiving an assertion from an executing process, wherein the executing process is

part of ~~integral to~~ an operating system and wherein the receiving an assertion module comprises modules for:

receiving an assertion request;

performing at least one of:

recognizing an assertion request type corresponding to the assertion request; or

determining a component that sourced the assertion request; and

accepting the assertion request for at least one of:

an assertion request of an enabled recognized assertion request type; or

an assertion request of a determined component which has assertion requests enabled;

recording the assertion; and

allowing the executing process to continue execution.

32-33. (Canceled)

34. (Previously Presented) The computer-readable medium of Claim 31 wherein the recording the assertion module comprises a module for recording a datum that includes at least one of:

type of assertion,

sequence number of the assertion,

time at which the assertion occurred,

identification of processor that produced the assertion,

identification of process that produced the assertion,

identification of the thread that produced the assertion,

text of the assertion,

stack trace,

source line containing the assertion, or

file name of the source containing the code that generated the assertion.

35. (Original) The computer-readable medium of Claim 31 wherein the recording the assertion module comprises a module for writing information regarding the assertion to a computer readable medium.

36. (Original) The computer-readable medium of Claim 31 wherein the recording the assertion module comprises a module for writing information regarding the assertion to a circular buffer.

37. (Previously Presented) The computer-readable medium of Claim 31, the instructions further comprising modules for:

accepting a command from at least one of a control console or a network connection; and

updating an enable condition for an assertion class according to the command.

38. (Original) The computer-readable medium of Claim 31, the instructions further comprising a module for generating an error report according to the recorded assertion.

39. (Original) The computer-readable medium of Claim 38, the instructions further comprising a module for dispatching the error report to a real-time assertion monitor.

40. (Previously Presented) The computer-readable medium of Claim 38 wherein dispatching the error report module comprises modules for:

retrieving an assertion violation parameter including at least one of:

type of assertion,

sequence number of the assertion,

time at which the assertion occurred,

identification of processor that produced the assertion,

identification of process that produced the assertion,

identification of the thread that produced the assertion,

text of the assertion,

stack trace,

source line containing the assertion, or

file name of the source containing the code that generated the assertion; and

generating a report file comprising page description statements according to the assertion parameter.

41. (Currently Amended) An apparatus for monitoring computer software comprising:

means for detecting an assertion from an executing process, wherein the executing process is part of ~~integral to~~ an operating system and wherein the means for detecting comprises:

means for ascertaining at least one of:

a type of an assertion request; or

a component that sourced an assertion request; and

means for ignoring the assertion request for at least one of:

a non-enabled ascertained assertion request type; or

a non-enabled ascertained component;

means for recording information pertaining to the assertion when it is violated; and

means for allowing the executing process to continue execution.

42-43. (Canceled)

44. (Previously Presented) The method of Claim 1 wherein the assertion request type is one of a group of defined assertion macro names.

45. (Previously Presented) The apparatus of Claim 11 wherein the assertion type is one of a group of defined assertion macro names.

46. (Previously Presented) The computer software monitoring system of Claim 21 wherein the assertion request type is one of a group of defined assertion macro names.

47. (Previously Presented) The computer-readable medium of Claim 31 wherein the assertion request type is one of a group of defined assertion macro names.

48. (Previously Presented) The apparatus for monitoring computer software of Claim 41 wherein the assertion request type is one of a group of defined assertion macro names.

49. (Currently Amended) A method for monitoring computer software comprising:

receiving an assertion from an executing process, wherein the executing process is part of ~~integral to~~ an operating system;

recording the assertion when the assertion is violated; and

allowing the executing process to continue execution.

50. (New) The method of claim 1, and further comprising differentiating between types of assertions by an amount of operating system resources to be used by the assertions.